Order Code RL32841

Border and Transportation Security: Possible New Directions and Policy Options

March 29, 2005

William H. Robinson, Jennifer E. Lake, and Lisa M. Seghetti
Domestic Social Policy Division

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
29 MAR 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Border and Transportation Security: Possible New Directions and Policy Options	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **David D. Acker Library and Knowledge Repository Defense Acquisition University Fort Belvoir, VA**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**24**	

Border Transportation Security: Possible New Directions and Policy Options

Summary

There is concensus that Border and Transportation Security (BTS) is a pivotal function in protecting the American people from terrorists and their instruments of destruction. The issue for Congress is how to achieve desired levels of security, while not compromising other important values in the process. This report addresses possible new approaches and policy options that might be explored by Congress to attain these goals. It is one of three CRS reports in a series that make use of analytical frameworks to better understand complex problems in BTS and to facilitate consideration of alternative policies and practices. (The first report in the series, CRS Report RL32839, *Border and Transportation Security: The Complexity of the Challenge*, analyzes the reasons why BTS is so difficult to achieve. The second report CRS Report RL32840, *Border and Transportation Security: Selected Programs and Policies*, discusses programs now in place. This report is the last in the series).

BTS plays an important role in the broader function of providing homeland security. The overall homeland security effort can be seen as a series of concentric circles or screens, with the outer screen being that of preventive efforts launched *outside* the country — before terrorists or their weapons can reach the country. The next screen is interdiction efforts at the border and in the transportation system. The continuum of activities then moves through progressively smaller circles ending with emergency preparedness and response. Congressional concern over homeland security began with broad-gauged efforts to learn more about the nature of the terrorist threat, and then moved to much more specific actions following the events of 9/11. Congressional interest in broader, more strategic approaches continues — which makes this review of possible new directions and policy options timely.

Both the complexity of the challenges at the border, and the realization that multiple points of vulnerability might be turned into expanded opportunities for interdiction, have given rise to the notion of a "layered" approach to security. The basic idea of layering is that multiple and overlapping measures applied at several points in the border security environment could be more successful than just more targeted measures. The problem in hardening a few selected targets is the rising expense of unit costs, increasing conflict with other goals, and/or inability to cover all conceivable risks posed by the shifting and opportunistic nature of terrorist tactics.

To pursue a layered approach to border and transportation security would mean applying some measure of security effort to each of the following points of vulnerability/opportunity: transportation staff, passengers, conveyances, access control, cargo and baggage, ports, and security *en route*. Several possible policy options are presented that flow directly from the framework presented in the three-part series of CRS reports. Before action is contemplated in any of these areas, however, it would be important to assess the priority of each step, its relative cost-effectiveness, and the level of intrusiveness and possible conflicts with other important social goals (e.g., privacy and civil liberties). This report will not be updated.

Contents

List of Figures

Border and Transportation Security: Possible New Directions and Policy Options

Introduction

Border and Transportation Security (BTS) is a pivotal function in protecting the American people from terrorists and their instruments of destruction. The issue for Congress is how to achieve desired levels of security, while not compromising other important values in the process. In a series of three reports, a strategic approach to BTS using a variety of frameworks to clarify objectives and help identify policy options is discussed. This final report builds on the analysis presented in the first two reports, and explores possible new directions and policy options that spring directly from the analytical frameworks contained in those reports. Before doing so, however, it is useful to place this set of activities in the broader context of overall Homeland Security efforts and to review the development of congressional concern and policy approaches up to this point.

The Role of Border and Transportation Security in Homeland Security

The homeland security effort can be seen as a series of concentric circles or screens, with the outer screen being that of preventive efforts launched *outside* the country. The continuum of activities to provide homeland security then moves through progressively smaller circles starting from more distant efforts to closer and more localized measures. Thus, the process starts with prevention abroad and ends with emergency preparedness and response at home:

- *Discovery and preventive intervention* of terrorist actions emanating from abroad before reaching the United States;
- *Interdiction* of dangerous people or things at the U.S. border and in the interior transportation sector;
- *Defense against catastrophic terrorism inside the United States* through law enforcement and domestic intelligence efforts;
- *Protection of critical infrastructure and the population*; and
- *Emergency Preparedness and response*.[1]

---

[1] For a more detailed discussion of this continuum, see CRS Report RL32840, *Border and Transportation Security: Selected Programs and Policies*, by Lisa M. Seghetti, Jennifer E. Lake, and William Robinson.

Congressional Concerns

Congressional concern with terrorism and border security was manifested early, following a series of terrorist attacks in the 1990s. The congressional response began with inquiries as to the nature of the terrorist threat and the commissioning of several studies, and was followed by specific, targeted measures to protect the nation following the events of 9/11. Congressional interest, however, continues in broader, more comprehensive approaches including efforts in the 108th Congress to respond to the report of the 9/11 Commission embodied in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA, P.L. 108-458). Congressional policy actions are summarized briefly below:

- *Broad efforts to understand the terrorist threat*. Starting in 1998, Congress stimulated the creation of three commissions to better understand the nature of the terrorist threat facing the nation. These included the Gilmore Commission, the Bremer Commission, and the Hart-Rudman Commission.[2]
- *Highly specific actions to protect against immediate threats*. Immediately following the airplane-based attacks of 9/11, early legislative action focused on airline security, visa and border security, and then moved on to maritime security.[3]
- *Structural and procedural changes to provide an effective framework for action*. Following the 9/11 attacks, Congress enacted legislation to create the Department of Homeland Security to provide a *structural* framework for subsequent action, and the USA PATRIOT Act to provide the *tools* needed for the new challenge to national security.[4]
- *Interest in broader, more comprehensive substantive approaches*. As evidenced in oversight hearings, Congress has been frustrated by the failure to more aggressively address other border and transportation security threats (including the need to create integrated terrorist watch-lists, and measures to address other modes of transportation — rail and mass transit, air cargo, trucking, and

---

[2] The official names and dates of creation of the Commissions are as follows: (1) Gilmore Commission, known officially as *The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*, created on Oct. 17, 1998 (P.L. 105-241); (2) Bremer Commission, known officially as *The National Commission on Terrorism*, created on Oct. 21, 1998 (P.L. 105-277); and (3) the Hart-Rudman Commission, known officially as *The U.S. Commission on National Security / 21st Century*, created on Sept. 2, 1999.

[3] The Aviation and Transportation Security Act (ATSA, P.L. 107-71) signed on Nov. 19, 2001; the Enhanced Border Security and Visa Entry Reform Act (P.L. 107-143) signed on May 14, 2002; and the Maritime Transportation Security Act of 2002 (P.L. 107-295) signed on Nov. 25, 2002.

[4] The Homeland Security Act was passed on Nov. 25, 2002 (P.L. 107-296). The USA PATRIOT Act, known officially as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, was passed on Oct. 26, 2001 (P.L. 107-56).

buses). These concerns were given a strong impetus by the Final Report of the 9/11 Commission, which highlighted the need for more strategic approaches to the terrorist threat, and are now expressed in legislative form in P.L. 108-458.

The evolution of congressional concern (moving from general to specific and back to broader concerns) makes this an opportune time to consider some possible policy frameworks that might shed additional light on the nature of the problem and possible new or enhanced policy choices. The next section of the report briefly summarizes the two earlier reports in the series that address the complexity of the challenge, as well as the programs and policies developed thus far to contribute to border and transportation security. The third section explores the idea of using a "layered" approach to protecting the nation — relying on multiple and overlapping policy actions on a number of fronts to increase the probability of interdicting bad people or bad things. The final section explores some ideas for possible new directions and policy options that spring directly from the analytical frameworks used in the report.

The Complexity of the Border Security Challenge and Selected Policy Tools Now in Use

The task of providing border and transportation security is complex both because of its scale and possible conflicts with other important national goals. The magnitude of the task is substantial — covering thousands of miles of land borders, millions of passengers, hundreds of airports and seaports, and millions of individual motor vehicles, rail cars, and cargo containers.[5]

The first possible goal conflict springs from the demands of security confronting the need for facilitating the essential travel and trade that are at the heart of continued economic growth. This reality leads to a redefinition of the task from one of pitting security vs. economic well-being to that of good border management. Good border management requires facilitating (and even expediting) the flow of desirable goods and people across our borders, while screening out dangerous people and material. The process of doing that is made more manageable if the border is envisioned not merely as a physical boundary but rather as a flexible concept that allows for the possibility that the border begins at the point where goods or people commence their U.S.-bound journey. The result of such a broader perspective is a significantly wider array of options for good border management.

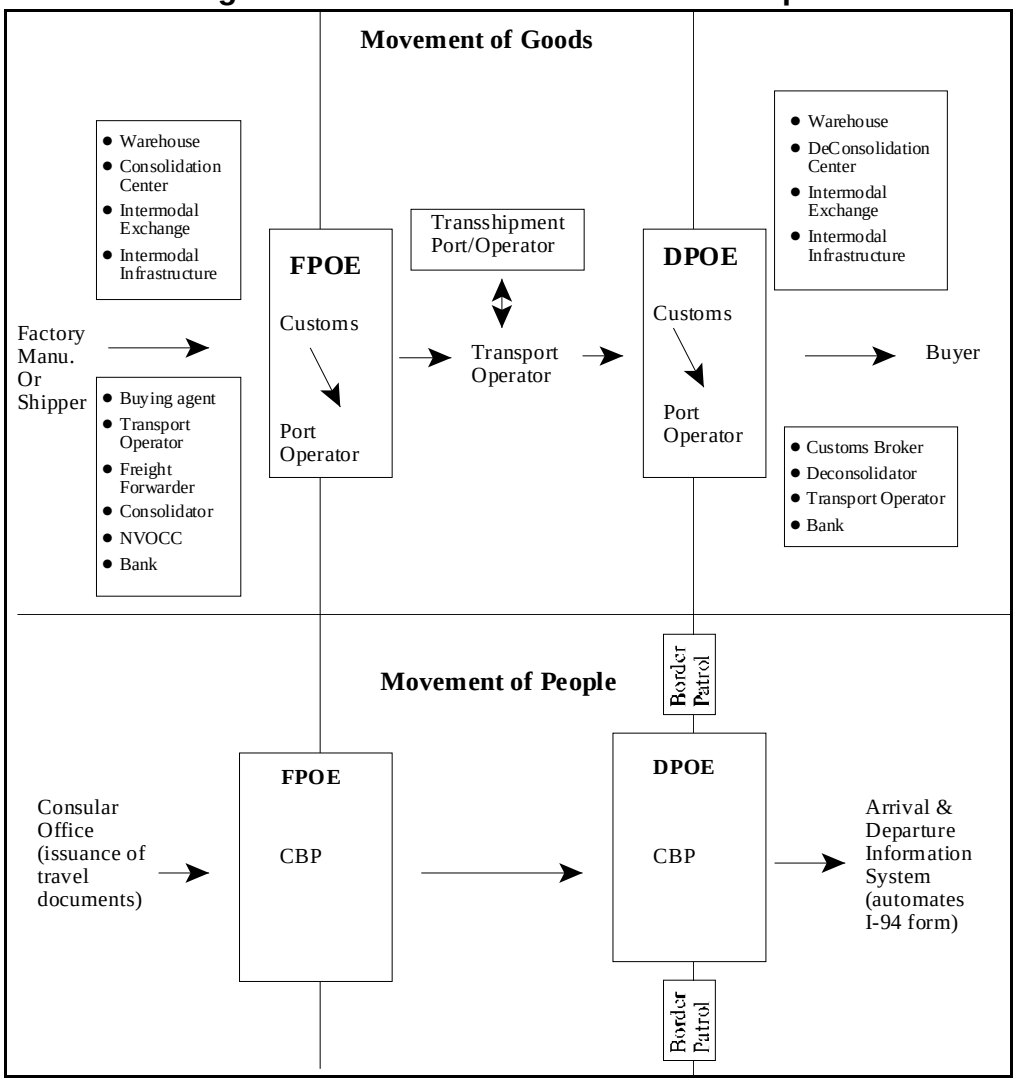
A companion report presents several graphical images of how this process might be envisioned. (See CRS Report RL32839, *Border and Transportation Security: The Complexity of the Challenge*.) That report blends the geographic dimension of the problem with the challenge of screening people, goods, and documents. It starts

---

[5] See the statement by Admiral James Loy, former Deputy Secretary of the Department of Homeland Security quoted in CRS Report RL32839, *Border and Transportation Security: The Complexity of the Challenge*, by Jennifer E. Lake, William H. Robinson, and Lisa M. Seghetti.

by identifying the paths that may be followed in moving from the source country to the United States, and then overlays the various points at which people, goods, and documents face the possibility of interception en route to the ultimate destination (the final destination inside the United States). The results are portrayed in **Figure 1** below. The figure should be viewed from left to right, moving from the foreign port of exit (FPOE) through a transit zone (illustrating the case where some goods or people might move through one or more intermediate countries en route), to the domestic port of entry (DPOE) — the final destination in the United States.

Figure 1. Movement of Goods and People



Source: CRS and CRS analysis of OECD figures in *Security in Maritime Transport*.
Note: FPOE = foreign port of exit, and DPOE = domestic port of entry.

In the process, exported goods may be handled by multiple intermediaries, people will follow several processes, and the necessary travel documents will pass through many hands. While designed to illustrate the multiple points where bad things can happen, the illustration also suggests that the multiple points of vulnerability in the shipping or travel process can also be seen as opportunities for

interception — and, if exploited, can actually increase the probability of interdiction of the bad things and bad people that we seek to intercept before they arrive at their intended targets.

The current programs designed to accomplish this interception are discussed more fully in the second report in this series: CRS Report RL32840, *Border and Transportation Security: Selected Programs and Policies*. These efforts can be summarized by using an analytical framework that highlights generic strategies that might be used to achieve greater border and transportation security:[6]

- Pushing the border outwards to intercept unwanted people or goods *before* they reach the United States (as in the Container Security Initiative and passenger pre-screening);
- Hardening the border through the use of technology (e.g., X-ray machines for examining cargo without opening the containers, radiation and explosives detectors, and unmanned aerial vehicles to monitor remote areas at the border);
- Making the border more accessible for legitimate trade and travel (faster passage for trusted travelers and cargo conveyors);
- Strengthening the border inspection process through more effective use of intelligence (terrorist screening data bases); and
- Multiplying effectiveness of interdiction programs through the engagement of other actors in the enforcement effort (including engaging Canada, Mexico, state and local law enforcement resources, and the private sector).

The realization that multiple points of vulnerability might be turned into expanded opportunities for interdiction has given rise to the notion of a "layered" approach to security. The basic idea of layering is that multiple and overlapping measures applied at key points in the border security environment could succeed where only more targeted measures might fail because of their rising expense, increasing conflict with other goals, or inability to cover all conceivable risks arising from opportunistic terrorist tactics.

"Layered" Approach to Border and Transportation Security

The concept of a layered approach to border and transportation security is gaining currency in policy discussions. The idea was cited in a security context in the so-called Gore Commission Report on aviation safety and security in early 1997.[7]

---

[6] See CRS Report RL32840, *Border and Transportation Security: Selected Programs and Policies*, by Lisa M. Seghetti, Jennifer E. Lake, and William H. Robinson for more details and a program-by-program discussion of the major efforts underway.

[7] *White House Commission on Aviation Safety and Security*, established by Executive Order 13015 on Aug. 22, 1996, and final report dated Feb. 12, 1997, p. 5. The commission was (continued...)

The commission stated the belief that "aviation security should be a system of systems, layered, integrated, and working together to produce the highest levels of protection."[8] An important pre-9/11 reference to "layering" was found in the Hart-Rudman Commission Report in 2001. The commission stated: "We believe that homeland security can best be assured through a comprehensive strategy of 'layered defense' that focuses first on prevention, second on protection, and third on response...." [9] This report discusses the concept of layered protection as applied specifically to border security, and offers a definition that is intended to translate the concept into something more concrete — with the goal of making it possible to be applied to actual programs and policy actions.

Background

The most recent advocacy of a layered approach comes from the 9/11 Commission Report issued in July 2004. Addressing the importance of passenger screening, the commission states: "The FAA set and enforced security rules, which airlines and airports were required to implement. The rules were supposed to produce a 'layered' system of defense. This meant that the failure of any one layer of security would not be fatal, because additional layers would provide backup security."[10] Later, the commission introduced a footnote specifically endorsing such a "layered" approach, and refers the reader to Dr. Stephen Flynn's latest work[11] in which he uses a household-based example of what layering would look like in a residential setting:

---

[7] (...continued)
created in the wake of concerns over the crash of TWA flight 800, and the earlier crash of Pan Am flight 103. One of the three charges to the commission was "to look at the changing security threat, and how we can address it...."

[8] Report of *White House Commission on Aviation Safety and Security*, p. 18. The notion of "layering" in the area of transportation *safety* has a history that stretches back to the 1970s. But this was an early instance of the idea being applied in the context of aviation *security*.

[9] The Phase III Report of United States Commission on National Security/21st Century ("Hart- Rudman" Commission), *Road Map for National Security: Imperative for Change*, (Washington, DC: GPO), p. 11. However, it should be noted that the concept of "layering" is applied to the entire area of *homeland* security, but is not discussed in depth.

[10] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, (Washington, DC: GPO, 2004), p. 83. (Hereafter *The 9/11 Final Commission Report.*) However, the Commission adds the important caveat that "Each layer must be effective in its own right. Each must be supported by other layers that are redundant and coordinated," p. 392. With respect to the effectiveness of the layers in place on 9/11, the Commission concludes: "But each layer relevant to hijackings — intelligence, passenger prescreening, checkpoint screening, and onboard security — was seriously flawed prior to 9/11. Taken together, they did not stop any of the 9/11 hijackers from getting on board four different aircraft at three different airports," p. 83.

[11] Stephen Flynn, *America The Vulnerable: How Our Government Is Failing to Protect Us From Terrorism*, (New York, N.Y.: HarperCollins Publishing, 2004). (Hereafter cited as Flynn, *America the Vulnerable*.)

> The simple act of locking a door with a conventional lock will deter most amateur thieves.... Returning to our case of securing a home, we might consider some additional ways to ward off burglars without trying to make conventional doors and windows burglar-proof. Since thefts often occur at night, we could consider installing automatic lights that are triggered when people approach. A dog on the premises will provide another measure of security. Add to this a sign posted on the front lawn that indicates the home is monitored by a security company. Finally the community could form neighborhood watch groups and post signs on the streets advertising this fact. Any of these measures might work only 60% of the time. But statistically, five 60% measures when placed in combination will raise the overall probability of preventing a burglary to 99%. In many instances, it may well be that the cost of all these measures is less expensive than trying to bolster any one or even two measures.[12]

Definition of a "Layered Approach" to Border Security

A truly operational definition would be applicable to the entire environment of border and transportation security, and would suggest specific action points and measures for added protection. The following is a provisional attempt to address that need:

> A "layered" approach to border and transportation security is a comprehensive strategy that identifies key points of vulnerability wherever they exist (including travelers, staff, cargo, vehicles, processes, documents, and locations) and turns them into targets of opportunity for interdiction. It provides a series of interdependent, overlapping, and reinforcing redundancies, designed to raise the odds that terrorist activity could be intercepted — also raising the risks and costs to terrorists, and serving both an interception and deterrence function.[13]

Layering speaks to three dilemmas of policy design in border and transportation security:

- The law of diminishing returns — i.e, at some point, the unit costs of any single measure become increasingly high as we attempt to push to higher levels of security;

---

[12] Flynn, *America the Vulnerable*, pp. 68-69.

[13] The 2002 report of the Council on Foreign Relations contains a reference that comes the closest to the definition posed here. The first recommendation under the title of "Make Trade Security A Global Priority" reads as follows: "Develop a layered security system that focuses on the entire logistics and intermodal transportation network rather than on an unintegrated series of tactics aimed at addressing vulnerabilities at arrival ports or at already congested land borders." Report of an Independent Task Force Sponsored by the Council on Foreign Relations, *America Still Unprepared — America Still in Danger*, 2002, p. 25.

- Heightened goal conflict — as tightened security begins to impede the legitimate flow of desired people and goods,[14] as well as resulting in possible incursions on privacy and civil liberties; and
- The opportunistic nature of terrorism — i.e, the more we harden one target, the more likely that terrorists will shift their attention to a softer target and/or use different means.[15] To reduce cost and risk of operations, terrorists desire to use targets and methods that have been used successfully before, can be easily taught and replicated, and have a high probability of success and impact. Frustrating any or all of these goals could lead to abandoning the operation.

A Layered Approach to Border and Transportation Security

Figure 1 illustrates that the security of people and cargo destined for the United States requires a complex set of policies that engage actors from each of the geographic zones (foreign governments, private sector actors, and U.S. government agencies). These relationships and policies must also take into consideration requirements unique to the different modes of transportation (air, vessel, truck, and rail). Policies could, for example, encompass the entire journey from the source zone to the destination zone; or policies could focus distinctly on a particular zone/place/actor in the journey. Or, as noted above, a layered approach may be employed that involves nearly all of the constructs identified in **Figure 1** (e.g., people, conveyances, cargo, places, routes, etc.)

Possible New Directions and Policy Options

To pursue a layered approach to border and transportation security would mean applying some measures of security effort to each of the following points of vulnerability/opportunity:

- *Staff authentication* — focusing on any staff involved with the transportation of people or shipment of goods;

---

[14] Stephen Flynn comments on the first two dilemmas in the following terms: "Our goal should not be to find fool-proof solutions for protecting the targets terrorists are most likely to strike. It is about identifying workable measures that are cost-effective and not disruptive. Then we need to string them together in such a way that each serves to reinforce the deterrent value of the other." Flynn, *America the Vulnerable*, p. 70. All of Chapter 3 "Security Maturity" addresses the layering notion.

[15] For a striking example of this tactical flexibility, see the *New York Times* article, which describes a joint FBI-DHS threat assessment. That assessment reportedly warns that Al Qaeda and other jihadist terrorists may be shifting their focus from commercial airliners (which still remain a serious target) to charter planes, helicopters, and other more vulnerable general aviation targets, as the commercial airline sector becomes more secure. The report goes on to note that "members of Al Qaeda appear determined to study and test new American security measures to 'uncover weaknesses,'" p. A-16. Eric Lichtbau, "Security Report on U.S. Aviation Warns of Holes," *New York Times*, Mar. 14, 2005, pp. A-1, A-16.

- *Passengers* — screening anyone traveling on any of the conveyances of concern;
- *Conveyances* (passenger or cargo) — monitoring the vessel, car, truck, plane, train used in conveying travelers or goods — including concern for the physical security of the conveyance itself;
- *Access control* — implementing a system to achieve and maintain control of the physical space where the conveyances or cargo are either stored, staged, maintained, repaired, loaded, or inspected.
- *Cargo and baggage* — screening whatever is placed on the conveyance, including cargo, as well as baggage associated with passengers;
- *Ports* (points of departure, transit, and entry) — encompassing all kinds of ports (airport, land port, sea port, rail yard/crossing), and involving physical security of the port itself, access control, and some kind of monitoring systems; and
- *Security en route* — maintaining the highest level of security throughout the system/between ports — reflecting that whatever security is achieved in the initial stages before or during the time when people or cargo leave the foreign port, must be maintained until the conveyance safely reaches the domestic port of entry and the intended recipient.

Looking at each of these targets of vulnerability and seeing them as opportunities suggest some possibilities for further policy exploration. The following are offered as brief illustrations of areas that might warrant further consideration based on the framework set out above. In many cases, actions have already begun, and the option would relate to acceleration or enhancements. In others, where new beginnings are envisioned, the options might entail further research or exploration.[16] However, it should be noted that action in any of these areas would need to be weighed against prevailing resource constraints and possible conflicts with other important societal goals (such as facilitating the legitimate flow of people and goods, and avoiding infringements on civil liberties and rights). With these qualifications, the following options might be explored as part of a layered approach to border and transportation security.

Staff Authentication

One early interception opportunity in the transportation process is to ensure that all transportation staff are whom they claim to be, and that terrorists do not gain access to, or gain control of, any part of the transportation system. The options below address this point of vulnerability/opportunity.

Secure Identification. Accelerate implementation of the experimental program for development of a Transportation Workers' Identification Credential

---

[16] For futher information on the status of existing border and transportation security efforts, see CRS Report RL32840, *Border and Transportation Security: Selected Programs and Policies*, by Lisa M. Seghetti, Jennifer E. Lake, and William H. Robinson.

(TWIC),[17] with enhancement of the screening process.[18] In spring of 2005, prototype versions of the TWIC were being tested in a variety of sites, involving 2,000-3,000 truck drivers, longshoremen, and other workers at the Ports of Los Angeles and Long Beach as well as at 33 other locations. The pilot program tests three different types of biometric identification (iris scans, fingerprints, and hand geometry). The plan is to apply a single standard to an estimated 5 million transportation industry workers at seaports, airports, chemical plants, and other protected facilities in the United States.[19] Next steps could include acceleration of the implementation of TWIC (particularly to maritime workers) and possible expansion to workers in all areas of transportation. Through international agreement, it may be possible to consider expanding secure identification to transportation workers from other countries.

Screening for All Staff. An option would be some level of screening for staff at all levels and points in the process, including office workers along the entire supply and shipping chain. In this sense, even clerks in shipping houses may represent some level of vulnerability, since they have the capacity to alter documents that disguise the real contents of shipments.

Passengers

Another key point in the process is to ensure that terrorists do not gain access to transportation systems and cross our borders and/or perpetrate an act of terrorism while on board. To add this layer of defense might involve the following.

Improved Terrorist Screening. Undertake improvements in terrorist screening databases. The 9/11 Commission recommends that "Every stage of our border and immigration system should have as part of its operations the detection of terrorist indicators on travel documents. Information systems able to authenticate travel documents and detect potential terrorist indicators should be used at consulates, at primary border inspection lines, in immigration services offices, and in intelligence and enforcement units."[20] This effort would start with expansion of intelligence efforts feeding into the databases, and would be enhanced by more sophisticated name recognition software (to reduce the number of false positive identifications). Finally, the entire effort could benefit from better integration of databases and other technical improvements for greater ease and speed of use at the border and by other immigration and law enforcement personnel.[21] The enhanced

---

[17] *The 9/11 Final Commission Report*, p. 392.

[18] For additional information on secure identification and access efforts for airports and aircraft, see CRS Report RL31969, *Aviation Security: Issues Before Congress Since September 11, 2001*, by Bartholomew Elias.

[19] See *The Journal of Commerce Online*, Nov. 17, 2004 at [http://www.joc.com/cgi-bin]. According to *CQ Homeland Security*, TSA is working with the Coast Guard to draft TWIC rules for maritime workers (Nov. 17, 2004).

[20] *The 9/11 Final Commission Report*, p. 385.

[21] See CRS Report RL32366, *Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6*, by William Krouse.

screening effort would also involve improved training for border security staff (see section on training, below).

Biometric Identifiers. One of the key recommendations of the 9/11 Commission was to expand the use of biometric identifiers as one of the more secure forms of identity authentication. The Commission noted that when people travel, they usually move through defined channels or portals:

> They may seek to acquire a passport. They may apply for a visa. They stop at ticket counters, gates, and exit controls at airports and seaports. Upon arrival, they pass through inspection points. They may transit to another gate to get on an airplane. Once inside the country, they may seek another form of identification and try to enter a government or private facility. They may seek to change immigration status in order to remain. Each of these checkpoints or portals is a screening — a chance to establish that people are who they say they are and seeking access for their stated purpose, to intercept identifiable suspects, and to take effective action.[22]

This effort would include continued research into the most effective biometric identifiers, assessment of their relative cost and feasibility of use, and the development of appropriate standards. It could also include research and investment in readers to increase the accuracy, speed, and efficiency of use at multiple portals.[23]

Screening for Other Modes of Transportation. Explore feasible and effective methods of screening for rail and transit passengers. While early passenger screening efforts understandably focused on air transportation passengers, the 9/11 Commission urged that efforts be made to expand coverage to other modes — especially passengers on rail and mass transit systems.[24] Referring to major vulnerabilities that still exist in cargo and general aviation security, the commission stated that "Opportunities to do harm are as great, or greater, in maritime or surface transportation."[25] Because of the need to maintain the free flow of people that is an essential feature in the effective functioning of these modes, passenger screening in this setting would require additional research and creative experimentation. But, given the threat made manifest in the 3/11 train bombings in Madrid in 2003, many experts believe further exploration of feasible screening methods is merited. The Intelligence Reform and Terrorism Prevention Act of 2004 [P.L. 108-458] also extended some form of screening to cruise ships and larger charter airplanes.[26]

---

[22] *The 9/11 Final Commission Report*, p. 385.

[23] For more information on this topic, see CRS Report RS21916, *Biometric Identifiers and Border Security: 9/11 Commission Recommendations and Related Issues*, by Daniel Morgan and William Krouse.

[24] See CRS Report RL32625, *Passenger Rail Security: Overview of Issues*, by David Randall Peterman; and CRS Issue Brief IB10135, *Transportation Security: Issues for the 109th Congress*, coordinated by John Frittelli.

[25] *The 9/11 Final Commission Report*, p. 391.

[26] P.L. 108-458, §4012(a) for charter aircraft and §4071 for cruise ships.

Training for Inspectors. Provide better training for border inspectors, in conjunction with augmented research on terrorist travel methods and document falsification techniques. This was an area highlighted in the 9/11 Commission final report (and especially in its supplementary volume on terrorist travel):

> We found that as many as 15 of the 19 hijackers were potentially vulnerable to interception by border authorities. Analyzing their characteristic travel documents and travel patterns could have allowed authorities to intercept four to 15 hijackers and more effective use of information available in U.S. government databases could have identified up to three hijackers.[27]

According to the commission, there were clear signs and markings on the travel documents used by most of the terrorists that would have linked them to terrorism, but that these telltale marks were the results of recent research and were not part of routine inspector training at the time.

Comprehensive Screening Throughout the Transportation Process. Explore ways to deny internal travel to those terrorists who have already entered the country — whether legally or illegally. The commission asserted that:

> Targeting travel is at least as powerful a weapon against terrorism as targeting their money. The United States should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility.[28]

The 9/11 Commission report suggests setting national standards for state-issued documents — including birth and death certificates, driver's licenses, etc.[29] That proposal was addressed in part in the Intelligence Reform and Terrorism Prevention Act of 2004, and has also been the subject of further legislation in the 109th Congress (H. R. 418). (H.R. 418 was passed in the House of Representatives on February 10, 2005).[30]

Conveyances

As part of the layering effort, attention could also be given to the actual means of transportation to ensure their safety and integrity. These steps could include:

Vehicle Inspection. Provide regular inspection of all transportation conveyances and their environments for possible terrorist tampering and/or planting of explosive devices. These inspections could include some strategic risk targeting, but would also benefit from random inspections as well (as discussed further below).

---

[27] *The 9/11 Final Commission Report*, p. 384.

[28] Ibid., p. 385.

[29] Ibid., p. 390.

[30] See CRS Report RL32754, *Immigration: Analysis of the Major Provisions of H.R. 418, the REAL ID Act of 2005*, by Michael John Garcia, Margaret Mikyung Lee, Todd Tatelman, and Larry M. Eig.

Trucks as a Special Focus. Pay special attention to trucks in the inspection process, especially those carrying hazardous material.[31] Trucks were used in the Embassy bombings in Africa, and remain a favorite delivery mechanism for large-scale explosives (whether using imported materials, transporting hazardous material, or modifying domestic materials as in the case of Oklahoma City or the first World Trade Center attack in 1993).[32] Steven Flynn also notes a weakness in the overall transportation system for short-haul (drayage) truckers, where there is a high-turnover rate, and consequent difficulty in providing adequate security clearances.[33] Flynn goes on to recommend the use of transponders to track the location and route of those vehicles transporting hazardous material. Some have gone beyond that to propose an automatic shutoff device for large rigs hauling such material. California has considered such a plan in the past, and may be re-examining the concept.[34] According to a report on research being done at the Lawrence Livermore National Laboratory, truck-stopping devices are being designed that could be used by road-side law enforcement officers to activate the air-brakes of a truck carrying hazardous cargo to bring it to a quick stop if it was thought to represent a terrorist threat.[35]

Access control

Ensuring the safety of transportation vehicles themselves is an essential step in the security process, but an important stage of this effort is to protect the environment of the protected vehicles.[36] This is especially problematic for rail and transit systems, which have long exposed open stretches along rail tracks. Some reasonable steps, might include:

---

[31] For additional information on the Hazmat issue, see CRS Issue Brief IB10135, *Transportation Security: Issues for the 109th Congress*, coordinated by John Frittelli.

[32] The *Homeland Security Monitor* (Sept. 20, 2004) cites a report from the private sector (the Security Director's Report) indicating that the "... threat from a car or truck bomb, particularly from one containing hazardous materials (HAZMAT) is the most significant terrorist vulnerability in the private sector...." The HSM goes on to state that "Indications that terrorists may have attained training for commercial driver's licenses (CDLs) with HAZMAT endorsement coupled with multiple suspicious surveillance incidents over the past six months have heightened concern that a vehicle bombing may be part of the next terrorist incident in the United States (DHS Warning)." See HSM, Sept. 20, 2004 at [http://www.homelandsecuritymonitor.com/docs/hsm092004.htm].

[33] Flynn, *America the Vulnerable*, pp. 67-68.

[34] "California Looks Anew at a Truck-Stopping Device," *New York Times*, Aug. 6, 2004, p. A10.

[35] *The San Francisco Chronicle*, Mar. 21, 2005, p. E-1. Similarly, the article cites related research at Lawrence Livermore that focuses on the use of continuous signals from antennas located on strategic buildings that could be used to stop the approach of any truck carrying hazardous or other threatening materials.

[36] For additional information on secure identification and access efforts for airports and aircraft, see CRS Report RL31969, *Aviation Security: Issues Before Congress Since September 11, 2001*, by Bartholomew Elias.

Enhanced Access Control. Explore protective steps like more guards, fencing, cameras, and sensors in places where transportation vehicles are based or through which they transit.[37] It could also include hardware and software that basically replace the traditional key to sensitive areas with an intelligent credential (badge or plastic card) which could be verified specifically to the user through a biometric check. Such enhanced access control could also provide a number of useful by-products, including a record of movement that could capture every instance of request for entry, grant of entry, denial of entry and other data; a record of personnel movement; asset protection; and flexible security.[38]

Cargo and Baggage

Aside from screening passengers, cargo and baggage have been significant sources of concern and the focus of many policy actions and additional proposals. Some additional measures to consider include:

Cargo Containers.[39] Enhanced focus on shipping containers. Many analysts have identified containers as an area of particularly high-risk.[40] While only about 5%

---

[37] For some of the problems in attaining access control, see U.S. Government Accountability Office, GAO-04-728, *Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls*, June 2004; and GAO-04-1062, *Maritime Security: Better Planning Needed to Help Ensure an Effective Port Security Assessment Program*, Sept. 2004.

[38] A report in June of 2002 by the U.S. Treasury Advisory Committee on Commercial Operations of the U.S. Customs Service (COAC) serves as a useful illustration of "Total Asset Visibility and Authentication" in the supply chain. This state would integrate technologies and provide: "... the loading of shipments in a secure facility, by authenticated personnel; verification of the contents of the shipment; securing the container in transit; transmitting the content information and manifest information to customs and other stakeholders upon loading; being able to identify container tampering, and allow customs to verify the integrity of the container and its contents in a non-intrusive manner at the port of entry." [U.S. Treasury Advisory Committee on Commercial Operations of the U.S. Customs Service (COAC). Border Security Technical Advisory Group, *Volume Two: Report on Access Control Technologies*, June 14, 2002, pp. 3-6.]

[39] See CRS Report RL31733, *Port and Maritime Security: Background and Issues for Congress*, by John F. Frittelli.

[40] There are many bad things and bad people that can be transported in a container measuring 8'x8'x40', which faces a relatively low rate of inspection. The screening percentage of cargo and containers ranges from 5% to 23%, with inspection rates of 22.6% of rail containers; 5.2% of sea containers; and 15.1% of trucks entering the country. CBP Commissioner Robert Bonner has testified that in 2003 across all modes, CBP is inspecting 12.1% of all cargo containers entering the country. See Testimony of Commissioner, Customs and Border Protection Robert C. Bonner, in U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Oversight of Transportation Security*, 108th Cong., 1st sess., Sept. 9, 2003 (Washington: Federal Document Clearinghouse, Inc.), p. 34. But there is a serious definitional issue here. Just what is an "inspection" and what does it mean to "screen"? There are different perceptions of both these concepts both in terms of basic definition and intensity. For more on this issue see CRS Report *Border and Transportation*

(continued...)

of these large containers are being screened, there are serious obstacles to detailed container screening. As a result, enhancement might be considered for existing processes of advanced targeting of those especially high-risk containers, screening early in the process (before the container is loaded onto the ship), scanning devices to detect contraband and radiation without opening the box, and smart-container technology to detect and note when the box is opened, and possibly using Global Positioning System (GPS) technology to track container location at any given point in time.[41] Such proposals respond at least in part to the vulnerability of cargo while in the transit zone (illustrated in **Figure 1**.)

Air Cargo.[42] Increase attention given to air cargo inspection.[43] Stephen Flynn provides a provocative statement on this topic: "Nevertheless, while the flying public is busy shedding shoes and bags at X-ray check-in points, the tons of air freight being loaded in the belly of most commercial airliners continues to fly the American skies virtually uninspected."[44] This concern led the 9/11 Commission to recommend that TSA require that each airliner have at least one hardened container in which to place any suspicious cargo.[45] Others suggest better oversight of and industry-wide standards for the "known shipper" program to ensure that the supply chain is truly secure, and that more random checks would be a useful supplement. Congress required an immediate tripling of cargo inspections for cargo on airline passenger planes in the FY2005 Appropriations Bill approved for the Department of Homeland

---

[40] (...continued)
Security: The Complexity of the Challenge, pp. 5-6, by Jennifer Lake, William Robinson, and Lisa Seghetti. However, even with greater definitonal precision, there are still serious limits as to how much inspection or screening of individual containers may be possible. Flynn notes that it would take five inspectors up to three hours to screen a single container, while a 910 foot container ship could contain 2,000-3,000 boxes, each stacked up to 11 containers high and only 18 inches apart — making inspection on the ship virtually impossible. Flynn, *America the Vulnerable*, pp. 87-88.

[41] Flynn, *America the Vulnerable*, pp. 87-88. Chapter 5 "What's in the Box?" addresses the container issue in depth, pp. 81-110. The possibility of moving toward implementation of the use of such a device was discussed in a news article that the Food and Drug Administration was expected to announce the placement of tiny radio antennas on millions of medicine bottles to prevent counterfeiting and fraud. ("Tiny Antennas To Keep Tabs On U.S. Drugs," *New York Times*, Nov. 17, 2004, pp. 1, 15). The article stated that the radio-tag technology is expected to spread to other uses such as accelerated checkout at the grocery store, finding lost luggage at airports, streamlining warehouse operations, protecting cargo, and tracking the location of passports or visas issued to visitors to the United States. While the radio tags cost only 20-50 cents, the readers and scanners needed to activate the information on the tags will cost several thousand dollars initially — but are expected to drop as the technology spreads.

[42] For more information on this topic, see CRS Report RL32022, *Air Cargo Security*, by Bartholomew Elias.

[43] See U.S. Government Accountability Office, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System*, GAO-03-344, Dec. 2002.

[44] Flynn, *America the Vulnerable*, p. 49.

[45] *The 9/11 Final Commission Report*, p. 393.

Security.[46] None of these efforts approaches the stringency of the 100% inspection proposal of Congressman Ed Markey (D-MA) in the 108th Congress.[47]

Rail Cargo. Expand use of fixed and mobile portal screening devices for explosives and radiation detection, as well as random inspections for other hazardous material. Flynn and others recommend a review of all rail routes that would take hazardous cargo through heavily populated areas, and re-routing them as necessary.[48] Recently, the City Council for the District of Columbia, passed a 90-day ban on shipments of hazardous materials through the nation's capital — the first such action by a local government.[49]

Ports, Terminals, and Inter-Modal Connections

"Vehicles at rest are vehicles at risk." While not completely safe while en route, transportation vehicles are most vulnerable when entering, leaving, or at rest in ports.

Sea Ports.[50] Enhance and expand maritime domain awareness efforts. Domain awareness makes use of radar, sonar, cameras, and direct observation to track all vessels entering or leaving the harbor on an integrated computer display, and link the vessels with cargoes and crews for possible inspection targeting and/or interception. It is also used to protect incoming and outgoing vessels from threats within the harbor or when approaching or departing. While well-developed in several ports, maritime domain awareness efforts might productively be expanded to more ports and improved — especially in light of the related concern about the potential threats posed by large shipping containers and large liquid natural gas conveyances.

Rail and Transit Terminals.[51] Strengthen security at rail and transit terminals. As noted earlier by the 9/11 Commission Report: "Surface transportation systems such as railroads and mass transit remain hard to protect because they are so accessible."[52] Yet, the "3/11" attacks on the Madrid rail system in 2003 and the Aum

---

[46] P.L. 108-334, signed Oct. 18, 2004.

[47] H.R. 2455 (108th Cong., 1st sess.), introduced on June 12, 2003.

[48] See, for example, Flynn, *America the Vulnerable*, p. 121.

[49] "90-Day Hazmat Ban is Passed," *Washington Post*, Feb. 2, 2005, p. B-1. However, the ban was followed one week later by a legal challenge by a major shipper, CSX. "CSX Challenges D.C. Ban of Rail Hazards," *Washington Post*, Feb. 9, 2005, p. B-3. For an overview of legal issues, see CRS Report RS22041, *Legal Issues Concerning State and Local Authority to Restrict the Transportation of Hazardous Materials by Rail*, by Todd B. Tatelman.

[50] For additional information on this issue, see CRS Report RL31733, *Port and Maritime Security: Background and Issues for Congress*, by John F. Frittelli.

[51] For background, see CRS Issue Brief IB10135, *Transportation Security: Issues for the 109th Congress*, coordinated by John Frittelli.

[52] *The 9/11 Final Commission Report*, p. 391. See also, U.S. Government Accountability (continued...)

Shinrikyo sarin gas subway attack in Tokyo on March 20, 1995 should leave no doubts as to the capabilities or the intent of terrorists to strike these targets. For passenger travel and transit systems, where accessibility and openness are prime goals, various analysts have suggested more extensive use of non-intrusive inspection (NII) technologies such as portal screening devices, "puffer" type explosive screening for passengers (recently tested in the New Carrollton station in the Washington metropolitan area and New York's John F. Kennedy airport), sensors for chemical and biological materials, bomb-sniffing dogs, frequent traveler IDs, and random checks of passengers and baggage en route.[53]

Connecting Points for Inter-Modal Transportation. Explore ways to strengthen security at the nexus points for multi-modal shipping as cargo moves from one conveyance to another (truck to container to ship to train to truck to delivery). This could include security for smaller pallets of goods (which fall short of constituting a full container) to ensure no tampering as cargo goes through the consolidation and de-consolidation phases.[54]

Port Design and Security. Explore the concept using port design to build security into the on-going processes of the port in a seamless manner. New designs could facilitate such essential security steps as in-line baggage screening, inspection

---

[52] (...continued)
Office, *Some Actions Taken to Enhance Passenger and Freight Rail Security, But Significant Challenges Remain*, GAO-04-598T, Mar. 23, 2004.

[53] CRS Report RS21893, *Passenger Rail Security: Overview of Issues*. See also "JFK Airport to Receive Walk-Through Explosives Detection Portal," *Homeland Security Monitor*, Oct. 26, 2004. In June 2004, Congressman Don Young (Chair of the House Transportation and Infrastructure Committee) introduced a bill in the 108th Congress (H.R. 4604) that would have provided "more than $1 billion for rail security, including $600 million to improve safety and security of rail tunnels used by Amtrak and various commuter lines." (*CQ Homeland Security*, June 18, 2004).

[54] There are many bad things and bad people that can be transported in a container measuring 8'x8'x40', which faces a relatively low rate of inspection. The screening percentage of cargo and containers ranges from 5% to 23%, with inspection rates of 22.6% of rail containers; 5.2% of sea containers; and 15.1% of trucks entering the country. CBP Commissioner Robert Bonner has testified that in 2003 across all modes, CBP is inspecting 12.1% of all cargo containers entering the country. See Testimony of Commissioner, Customs and Border Protection Robert C. Bonner, in U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Oversight of Transportation Security*, 108th Cong., 1st sess., Sept. 9, 2003 (Washington: Federal Document Clearinghouse, Inc.), p. 34. But there is a serious definitional issue here. Just what is an "inspection" and what does it mean to "screen"? There are different perceptions of both these concepts both in terms of basic definition and intensity. For more on this issue see CRS Report *Border and Transportation Security: The Complexity of the Challenge*, pp. 5-6, by Jennifer Lake, William Robinson, and Lisa Seghetti. However, even with greater definitonal precision, there are still serious limits as to how much inspection or screening of individual containers may be possible. Flynn notes that it would take five inspectors up to three hours to screen a single container, while a 910 foot container ship could contain 2,000-3,000 boxes, each stacked up to 11 containers high and only 18 inches apart — making inspection on the ship virtually impossible. Flynn, *America the Vulnerable*, pp. 87-88.

at rail sidings, and easier access in areas of heavy traffic and bottlenecks (e.g., the Ambassador Bridge at the Detroit-Windsor connection, and other congested land-border ports).[55] The challenge is often to make better use of very limited space, and it may take re-design efforts to achieve higher levels of security effectiveness. A design initiative could involve all kinds of ports and terminals (airport, seaport, rail and transit).

Security *en Route*/Asset Tracking

Total system security requires maintaining the high levels of security at each stage of the journey, through intermediate ports of call, and throughout the system until the destination is reached and the goods or people safely reach the intended destination.

Vulnerability of the Transit Zone. Consider the adoption of special efforts to assure security of passengers and cargo as they move through the highly porous — and vulnerable "transit zone." (See **Figure 1**.) One possibility is exploring the use of multi-modal security devices for cargo, including "smart containers" and transponders.

Cross-Cutting Measures

There are a number of potential actions that would cut across modes of transportation and/or points of vulnerability or opportunity. The following policy options present the potential for multiple payoffs in terms of security.

Better Targeting of Terrorists and Dangerous Materials. Explore methods for better targeting of both passengers and cargo. This could involve a blend of sophisticated and directed targeting, with an additional complementary component of random inspections. The goal would be to achieve the greatest level of confidence concerning the contents of a container or the identity of the individual seeking entry, in order to isolate and interdict high-risk people and goods. The ability to intercept high-risk people may be dependent on a combination of biometric identifiers, accelerated implementation of the US-VISIT program, better integration of terrorist watch lists, better training of border inspectors, and use of screening at several points in the transportation process. The ability to successfully target high-risk containers is dependent upon similar needs, with the crucial addition of information regarding which containers are most likely to contain contraband. Both

---

[55] One example of the use of integrated security design can be seen at Terminal six at the JFK airport in New York City. Since many airports were originally designed in the 1960s or1970s, many are looking to modernize their facilities to incorporate security initiatives into the basic structure. See, for example, "Airport Security Demands Give Wing to Architectural Boom," *CQ Homeland Security*, Nov. 11, 2004. Efforts include building in-line baggage screening systems and kiosks for self-service checks under the US-VISIT program. Such terminal features are being considered for airports in a variety of geographical locations including Harrisburg, PA, Atlantic City, NJ, San Jose,CA, Rochester, NY and Santa Barbara, CA. A cited example of good design for a *land port* can be found at Douglas, AZ.

of these processes require better use of intelligence. They also require an attempt to avoid predictability in whatever we do to make it less likely that terrorists can take evasive actions based on second-guessing our targeting system. (See below).

Benefits of Random Inspections as a Supplement to Targeting. Make systematic use of random changes in inspection targets and procedures. Random changes and random inspections are useful supplement to targeting, in order to determine what you don't know — in terms of identifying gaps in present algorithms for setting targets. It also increases risks for terrorists, who may be studying the inspection process carefully in order to exploit any predictable patterns to avoid interdiction.[56] A good example of using random principles is found at the land border port between Mexico and the United States at the Douglas, AZ port. This port uses sophisticated (and automated) algorithms to randomly switch inspectors from one lane to another, as well as change targets for inspection — and does so at random intervals, using a secure communication system for the inspectors.

Strategic Planning: Red Teams and War Games. Consider the expanded use of "Red Teams" and war-gaming. These concepts are borrowed from both the national security and intelligence fields, and are related functionally. The use of Red Teams involves gathering experts in the security field and various potentially vulnerable sectors to creatively explore vulnerabilities and suggest ways in which attacks might be feasible. War games involve taking the scenarios developed by the Red Teams and determining ways to defeat the attack efforts. This path was cited approvingly by the 9/11 Commission in the following graphic example. The commission noted that such techniques have been used by the military for many years, revealing that the North American Aerospace Defense Command (NORAD) had run an exercise that "postulated a hijacked airliner coming from overseas and crashing into the Pentagon." The exercise was terminated because of the exigencies of the *Korean War*. The commission identified the four elements common to this type of contingency planning as "(1) think about how surprise attacks might be launched; (2) identify telltale indicators connected to the most dangerous possibilities; (3) where feasible, collect intelligence on these indicators; and (4) adopt defenses to deflect the most dangerous possibilities or at least trigger an early warning."[57] The first step represents the Red Team portion of the process, and the fourth step is the war-gaming phase. The intervening stages are used to target intelligence to inform the entire response process. The notion of "Red Teams" was specifically endorsed in the Bush Administration's National Strategy for Homeland

---

[56] For a striking example of this tactical flexibility, see the *New York Times* article, which describes a joint FBI-DHS threat assessment. That assessment reportedly warns that Al Qaeda and other jihadist terrorists may be shifting their focus from commercial airliners (which still remain a serious target) to charter planes, helicopters, and other more vulnerable general aviation targets, as the commercial airline sector becomes more secure. The report goes on to note that "members of Al Qaeda appear determined to study and test new American security measures to 'uncover weaknesses,'" p. A-16. Eric Lichtbau, "Security Report on U.S. Aviation Warns of Holes," *New York Times*, Mar. 14, 2005, pp. A-1, A-16.

[57] *The 9/11 Final Commission Report*, p. 346.

Security.[58] More recently, the Red Team technique was also endorsed by the 9/11 staff group charged with aviation and transportation security, in an early version of its draft report to the Commission.[59]

Multi-Purpose Detection Technology. Expand research and development efforts to develop better and more flexible detection devices for radiation and explosives that are capable of working across transportation systems.[60] In terms of explosives detection, the ability to use NII technology to detect explosives carried by a passenger at a distance could have a very high payoff in the crowded setting of rail and transit terminals.[61] The 9/11 Commission stated that "The most powerful investments may be for improvements in technologies with application across the transportation modes, such as scanning technologies designed to screen containers that can be transported by plane, ship, truck or rail. Though such technologies are becoming available now, widespread deployment is still years away."[62]

As noted above, this is not intended as a comprehensive inventory of all steps that could be considered, nor is it a series of recommendations. The examples cited here flow directly from the frameworks used above and offer a few *illustrative options* that might be worth further exploration.

---

[58] *National Strategy for Homeland Security*, Office of Homeland Security, July 2002, Washington, DC, pp. viii, 19.

[59] The study was only recently officially published. Prior to its release, there was some considerable discussion of it in the trade press by many who had seen the draft version of the report. See, for example, *Govexec.com Daily Briefing*, July 23, 2004 and *Homeland Security Monitor*, Sept. 10, 2004. They quote the staff recommendation identically as follows: "Congress should create independent 'Red Teams' outside of TSA and DHS for the covert testing of all transportation modes." While there was no direct reference to "Red teaming" in the final redacted version of the staff report, unredacted footnotes numbered 604, 607, and 610 all refer to the absence of "Red Team" exercises at Logan and Newark airports in the two years preceding 9/11. All the text to which the footnotes refer has been redacted. However, the simple existence of "Red Teams" could not possibly be the reason for redaction, since the concept is included in the National Strategy for Homeland Security, and the 9/11 Commission heard public testimony from the leader of several FAA Red Teams. See *Statement of Bogdan Dzakovic to the National Commission on Terrorist Attacks on the United States* (May 22, 2003). Cited at [http://www.globalsecurity.org/security/library/congress/9-11_commission/030522-dzakovic], accessed on Feb. 27, 2005.

[60] Flynn, *America the Vulnerable*, p. 122.

[61] Charles McQueary (Undersecretary of DHS for Science and Technology) stated that DHS was seeking devices capable of detecting explosives on an individual 100 yards away. GOVEXEC.com's *Daily Briefing*, June 14, 2004.

[62] *The 9/11 Final Commission Report*, p. 392.

Conclusion

The goal is to find more effective ways to promote better border management. This effort is complicated by the many potential goal conflicts that can arise in seeking greater security, while at the same time trying to pursue other important national goals like promoting economic growth, assuring freedom of movement to law-abiding citizens and allies, and protecting privacy and civil liberties. Pushing too hard on any one of these goals may make it too expensive, both in terms of resource costs, but also in losses imposed on other important social goals.

One possible path to facilitate this delicate balancing act is to pursue the "layered" approach recommended by the 9/11 Commission and other BTS analysts over the years. Such an approach would mitigate over-reliance on any one policy action, yet holds out the possibility of achieving a higher level of security *cumulatively* by spreading actions over many areas to enhance the odds of either interdicting or deterring terrorist activity wherever it may occur. It also addresses the dilemma of terrorist opportunism, which afflicts preventive efforts that are more concentrated. As fast as we secure one area through a concentration of resources, the terrorists have shown themselves to be remarkably adaptable in seeking other softer targets (in effect, finding the weakest link in the defensive chain and attacking it, instead of the newly hardened target).

Whether policymakers wish to follow the layering strategy discussed above, or pursue a more targeted approach, the options identified above may constitute a useful point of departure for possible actions to consider. Under any circumstances, the following criteria (in the form of policy questions) may be useful in evaluating how far to take any single action:

- What are the relative priorities for action in the near term?
- Does the action yield security benefits that outweigh possible social or economic costs?
- Is the step being taken in the least intrusive manner consistent with achieving the objective?
- Are incursions on privacy and civil liberties taken into account, minimized, and accompanied by appeals processes for any violations?
- In what ways will the steps under consideration interact with others in the security process to provide higher cumulative security